Wat doen we?
Bestanden en schijven definitief overschrijven

Waarmee?
Eraser en Darik's Boot and Nuke

Hoelang?
Een halfuurtje

Moeilijkheid?


Gegevens écht wissen
In de versnipperaar

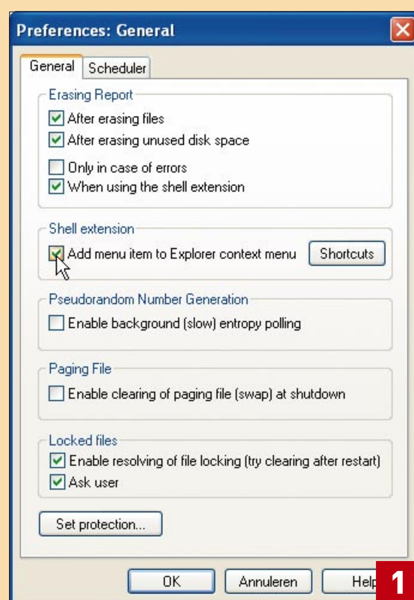
Je bent van plan om je oude pc te verkopen of weg te schenken, maar je wil er absoluut zeker van zijn dat niemand nog aan je gegevens kan? Voor zulke situaties schieten de prullenmand of een normale schijfformattering tekort. CEDRIC MESKENS

Je pc gaat binnenkort naar iemand anders en dus neem je je voorzorgen. Eerst en vooral zorg je voor een betrouwbare back-up van alle belangrijke gegevens, waarna je alle partities op de harde schijf herformatteert. Dat lijkt een solide methode, maar jammer genoeg garandeert dat helemaal niet dat alle gegevens effectief weg zijn. Bij zo'n herformattering wordt doorgaans namelijk alleen maar de bestandsindex – de fichebak zeg maar – leeggemaakt en blijft het eigenlijke datagebied onaangeroerd. Met speciale software als R-Studio www.r-studio.com zijn die gegevens alsnog weer op te vissen.
Ook het wissen van gegevens via de Verkenner is allesbehalve onherroepelijk, zelfs niet als je daarna de prullenbak leegmaakt. Een keur aan undelete-tools staat immers te trappelen om ook die data weer boven water te halen.
Om gegevens definitief te verwijderen, moet je ze met een (willekeurige) bitreeks overschrijven of 'shredden' (wat zoveel betekent als versnipperen). In deze workshop stellen we je twee verschillende 'shredders' voor: Eraser (waarmee je gegevens ook selectief kan shredden) en Darik's Boot and Nuke (voor het shredden van complete partities).

Selectief overschrijven

STAP 1 / ERASER INSTALLEREN

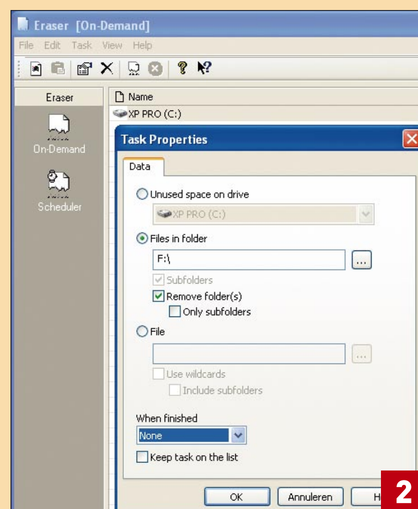
Eraser, een van de beste shredders, is openbronsoftware en dus gratis. Hij werkt in nagenoeg alle Windows-versies. Je kan de tool downloaden op www.heidi.ie. De installatie verloopt rechttoe rechtaan; na afloop vind je het programma terug bij **Alle programma's**, **Eraser**, **Eraser**. Start het programma op en overloop even de opties via het menu **Edit**, **Preferences**, **General** (zie afbeelding 1). Plaats je hier een vinkje bij **Add menu item to Explorer context menu**, dan kan je voortaan geselecteerde bestanden shredden via de Verkenner: je hoeft de selectie dan maar met de rechtermuisknop aan te klikken en **Erase**, **Yes** aan te klikken.



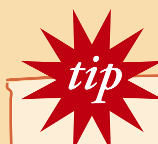
Kijk eerst alle instellingen van Eraser even na.

STAP 2 / TAAK UITVOEREN

Tijd nu om Eraser op te zadelen met een eerste taak. Klik in het linkerpaneel op het pictogram **On Demand**, open het menu **File** en kies **New task**. Op het tabblad **Data** heb je drie mogelijkheden. Wil je ongebruikte ruimte shredden – waar mogelijk nog oude gegevens verscholen zitten – stip dan **Unused space on drive** aan en verwijs naar de gewenste stationsletter. Met de tweede optie, **Files in Folder**, overschrijf je de complete inhoud van een bepaalde map (zie afbeelding 2). Plaats een vinkje bij **Subfolders** als je ook alle onderliggende mappen wil shredden. De derde optie **File** is bedoeld voor het shredden van specifieke bestanden. Bevestig met **OK**. De taak verschijnt nu in de lijst. Om die effectief uit te voeren, klik je erop met de rechtermuisknop en kies je **Run**. Is het je bedoeling om regelmatig dezelfde shredtaak te laten uitvoeren, dan plan je die beter in. Klik in het linkerpaneel eerst op **Scheduler** en creëer dan een nieuwe taak. Je zal merken dat het dialoogvenster er een nieuw tabblad (**Scheduler**) heeft bijgekregen, waarop je het tijdstip en de frequentie kan instellen.



Baken heel nauwkeurig het terrein af dat je wil shredden!

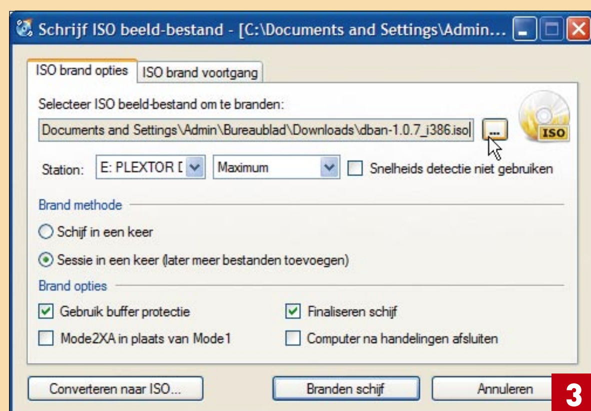


Wil je veel wissen, dan kan je de pc ***zichzelf laten uitschakelen*** *na afloop. Selecteer 'Shutdown system' bij 'When finished'.*

Hele partitie overschrijven

STAP 3 / ISO-BESTAND NAAR CD BRANDEN

De eveneens gratis tool Darik's Boot and Nuke (DBAN) vind je in twee verschillende versies op www.dban.org. De ene laat zich omtoveren tot een opstartbare cd/dvd, de andere is bedoeld om uit te voeren op een diskette of usb-stick (deze laatste versie kan je ook vanuit Eraser opstarten: ga naar **Alle programma's**, kies **Eraser**, **Create Nuke Boot Disk** en volg de instructies). Wij kiezen voor een opstartbare cd, omdat dat het gemakkelijkste is.
Download eerst het ISO-bestand van amper 2 MB en brand dit bestand vervolgens naar een cd. Bijvoorbeeld met de gratis tool CDBurnerXP www.cdburnerxp.se, waar je **Brand ISO beeldbestand** kiest en naar het gedownloade **ISO**-bestand verwijst (zie afbeelding 3). Na afloop beschik je dan over een cd. Daarmee start je de pc op die je wil leegmaken. Mogelijk moet je hiervoor wel nog de opstartvolgorde in het bootmenu (op te roepen met een sneltoets als F9) of het **BIOS** aanpassen. Raadleeg hiervoor de handleiding bij je moederbord.



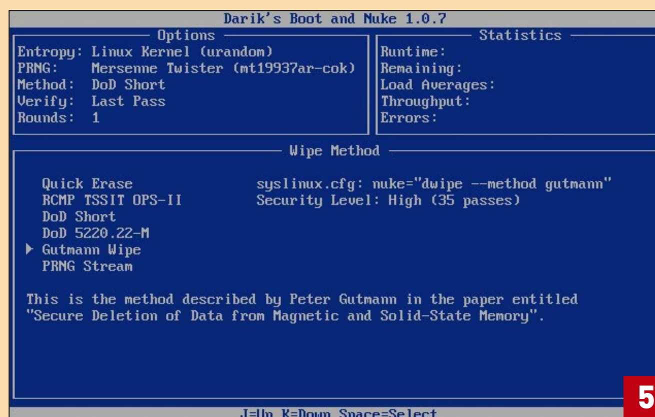
Van ISO naar cd: een kwestie van minuten.

STAP 4 / PROGRAMMA UITVOEREN

Zodra je je computer met deze cd hebt opgestart, verschijnt de bootprompt. Ben je er honderd procent zeker van dat alle media die op deze pc zijn aangesloten, mogen worden geshred, tik hier dan het commando `autonuke` in en bevestig met **Enter**. De tool begint dan zonder meer aan zijn vernietigende doortocht. Of druk eerst op **F3** en kies vervolgens een van de opgelijste commando's (waaronder `dod` en `gutmann`) om alle aangesloten media met een welbepaald algoritme uit te voeren.

STAP 5 / GEAVANCEERD WISSEN

Druk je bij de bootprompt gewoon op de **Enter**-toets, dan beland je in een min of meer grafische omgeving, van waaruit je DBAN interactief kan aansturen. Zo krijg je een overzicht van alle aangesloten media. Met behulp van de toetsen **J** en **K** kan je door deze lijst bladeren (zie afbeelding 5). Druk je bij een geselecteerde medium op de spatiebalk, dan verschijnt het woord [wipe] links van het medium: dat is nu gemarkeerd voor een shredoperatie. Met **F10** zet je deze operatie effectief in gang. Voor de techneuten onder ons: het is ook perfect mogelijk om zelf aan te geven hoe het shredden precies moet verlopen. Druk je op de letter **P**, dan kan je uit twee verschillende 'pseudo random number generators' kiezen – met de spatiebalk selecteer je een optie en keer je automatisch terug naar het vorige venster. Via de letter **M** of de komma op jouw toetsenbord komen maar liefst 6 verschillende shredalgoritmes aan je vingertippen (zie kaderstukje), met de letter **R** bepaal je hoeveel keer DBAN dit algoritme moet doorlopen en met **V** geef je te kennen of de tool moet nagaan of de gegevens wel degelijk zijn overschreven. Het spreekt vanzelf dat de duur van de hele operatie sterk zal afhangen van je instellingen. ♦



DBAN laat zich (via het toetsenbord) nauwgezet aansturen.



Algoritmes instellen

Zowel Eraser als Darik's Boot and Nuke laten je de toegepaste shredmethode nauwkeurig instellen. Bij Eraser vind je deze algoritmes via het menu **Edit**, **Preferences**, **Erasing**, terwijl je bij Boot and Nuke de juiste methode instelt via de letter **M** (zie stap 5). Typische algoritmes zijn onder meer die van het Amerikaanse ministerie van Defensie (Department of Defense, DoD). Bij DoD 7-pass bijvoorbeeld worden data zevenmaal overschreven. Een van de grondigste algoritmes is die van Gutmann, die de gegevens maar liefst 35 keer overschrijft.